Darknets and Ransomware

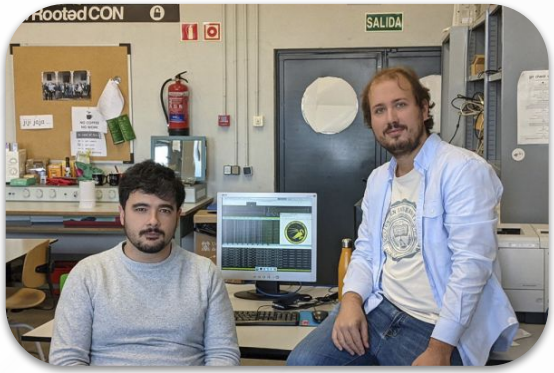
carlos.cilleruelo@byronlabs.io

Byron Labs

Information Security Research Lab
Universidad de Alcalá

BYRON LABS

Universidad de Alcalá



Ransomware

- Malware specifically designed to encrypt data on a device
- Data on a device is encrypted but the key is not given to the user
- If the user wants the key, he has to pay a ransom
- Usually, this ransom is paid in cryptocurrencies
- **If we do not have backups, we have lost the data**

POLICY \ TECH \ CRYPTOCURRENCY

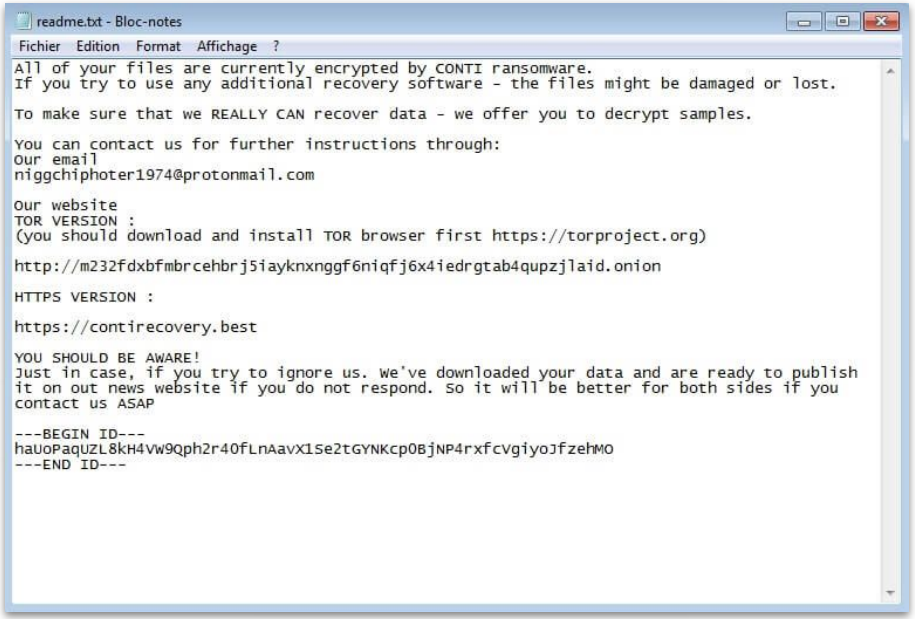
US Treasury says ransomware payouts in 2021 could top entire past decade

The top 10 hacker groups are tied to $5.2 billion in transactions

By Mitchell Clark | Oct 15, 2021, 6:46pm EDT

Ransomware


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy


readme.txt - Bloc-notes
Fichier Edition Format Affichage ?
All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.
To make sure that we REALLY CAN recover data - we offer you to decrypt samples.
You can contact us for further instructions through:
Our email
niggchiphoter1974@protonmail.com
Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)
http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion
HTTPS VERSION :
https://contirecovery.best
YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us ASAP
---BEGIN ID---
haUoPaqUZL8kH4Vw9Qph2r4OfLnAavX1Se2tGYNKcpOBjNP4rxfcVgiyoJfzehMO
---END ID---

Ransomware

NEWS

Spora Ransomware Provides 24/7 Customer Support To Victims!

By Harsh — On Feb 7, 2017

4 WTF is this?? and what is Bitcoin???

Could you check video on Instruction field?

A I got hit with this virus on the 3rd, now today it looks like the files changed. Are you also stopper@india.com, or is that a second ransomware?

We are only Spora Ransomware, no other ransomwares we can help

Gifted free decode for 798182B07B5530.
Please, make a review (with screenshots, payment details, decryption process) on site: http://bit.ly/2ky4Eb2

And few others that you will find.
Please, make a truthful review as it was.
Thank you

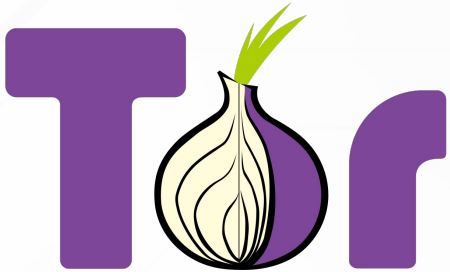
7 ok, now i will make some screenshots for proofs. And copy link to site. Thanks.

E Both of my computers have been infected by this. I was able to piece together the price for the first one in bitcoins but my other computer just showed up as being infected too. I will pay the full restore fee, but I dont think I could get the bitcoins in only 3 days, especially starting from scratch.

No problem. We disabled deadline for you. Pay asap, please. After this, left a review on http://bit.ly/2ky4Eb2 and we will send you back some bitcoins

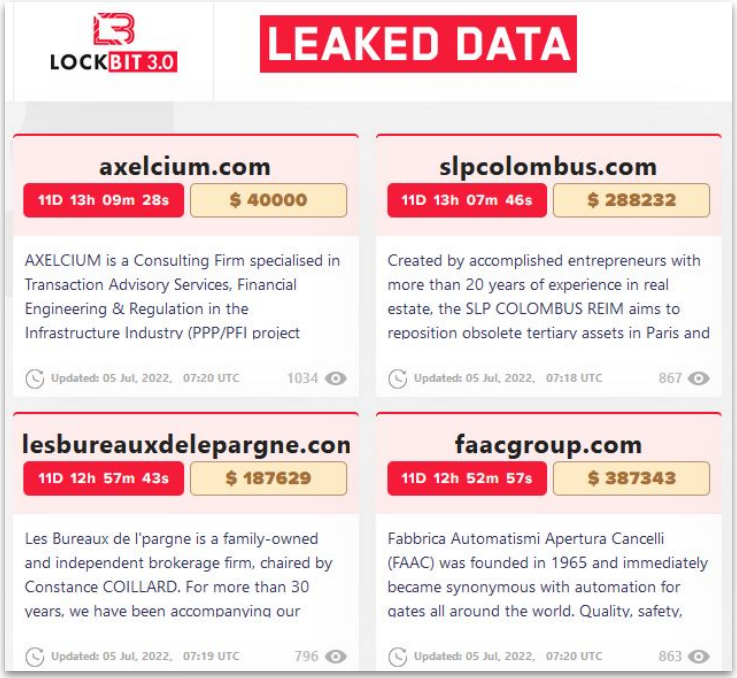
Evolution of the modus operandi

- Changes in modes of extortion information theft
- Now several ransomware groups steal the information of companies
- Encrypt and threat to publish this information



Evolution of the modus operandi

- Use of darknets to publish stolen information
- Contact with “clients” through Tor hidden services

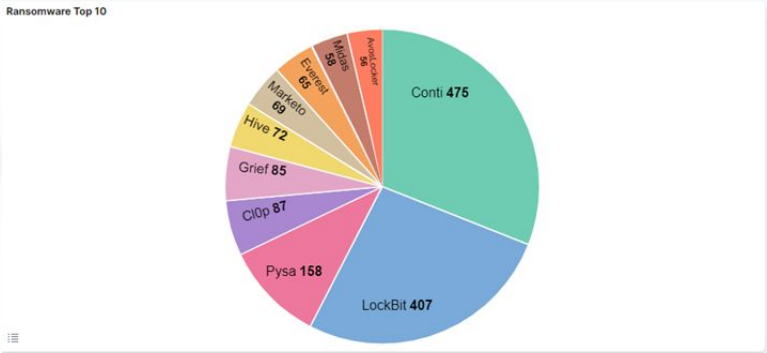


Evolution of the modus operandi

- Changes in modes of extortion information theft
- Now several ransomware groups steal the information of companies
- Encrypt and threat to publish this information

Analysis

- We monitored and download data from 31 ransomware groups in 2021
  - Now we analysing 2022 to data



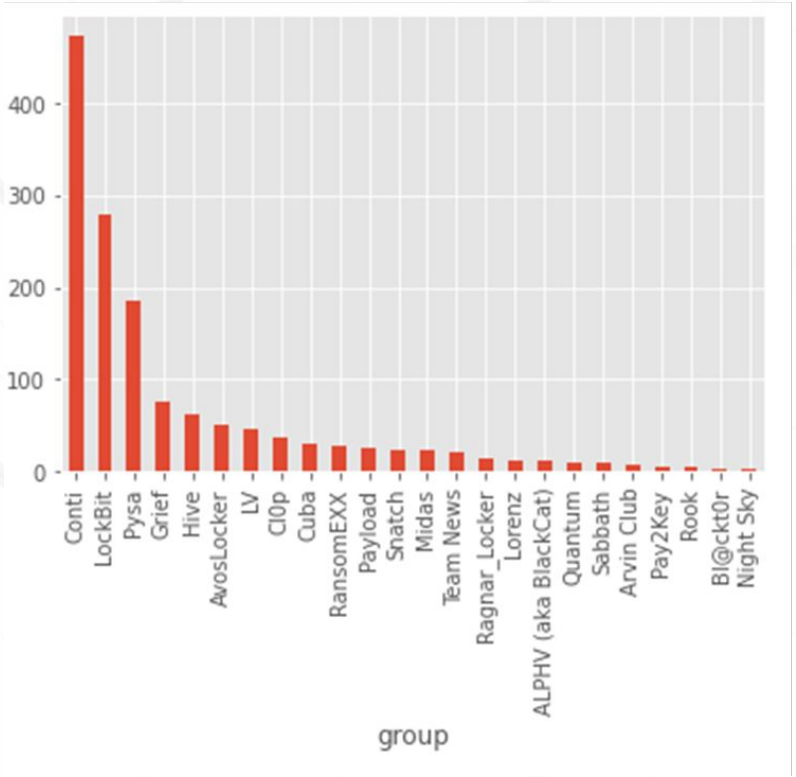
Ransomware Victims

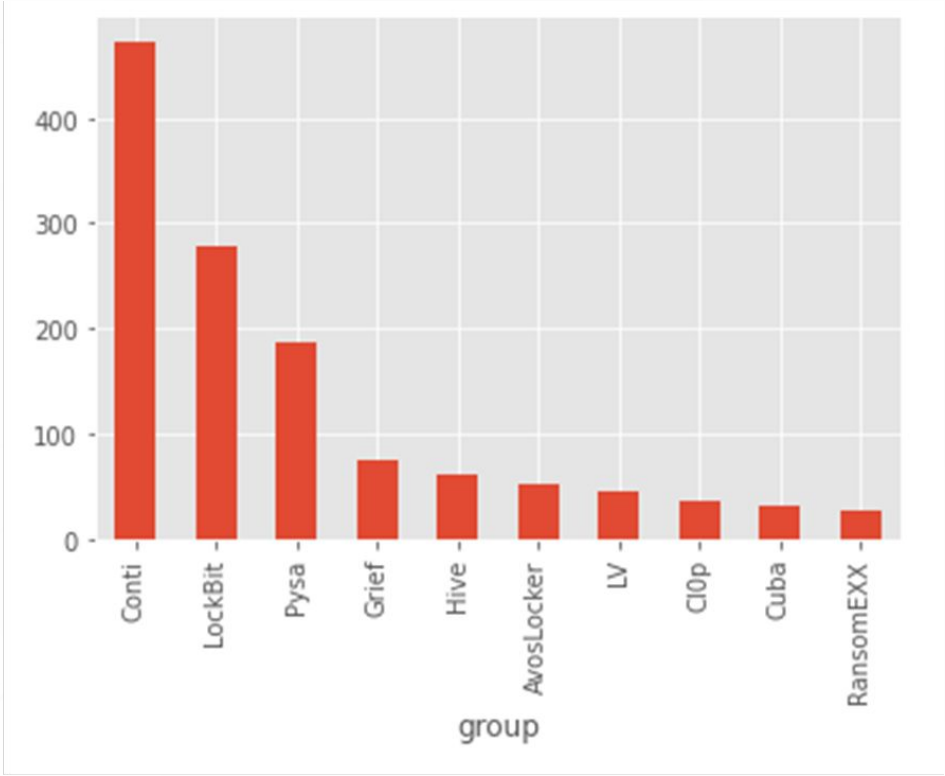
Export

Company	Company Link	Tor Link	Group	Date	Count
ALEXIM.COM	http://alexim.com	http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/alexim-com	Cl0p	2022-02-14	1
ALTERNATIVETECHS.COM	http://alternativetechs.com	http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/alternativetechs-com	Cl0p	2022-02-14	1

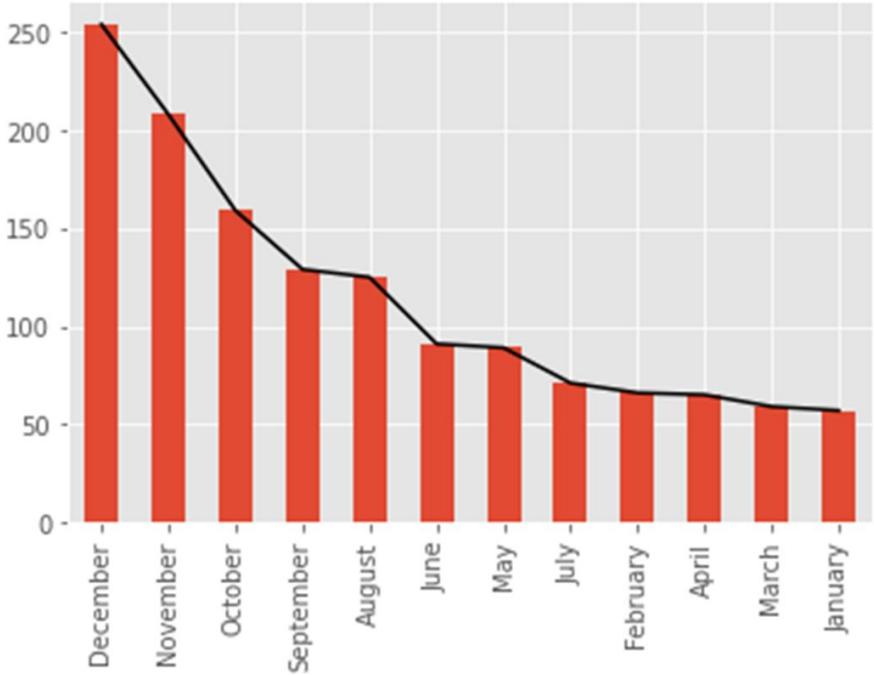
31 monitored groups in 2021

Most active groups

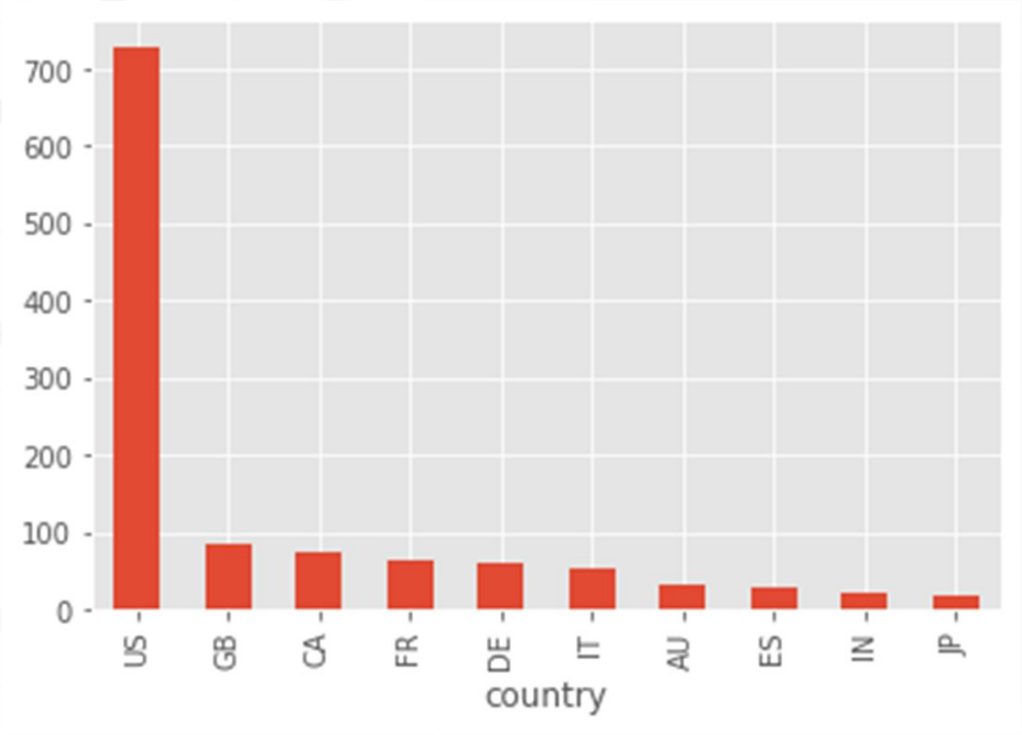




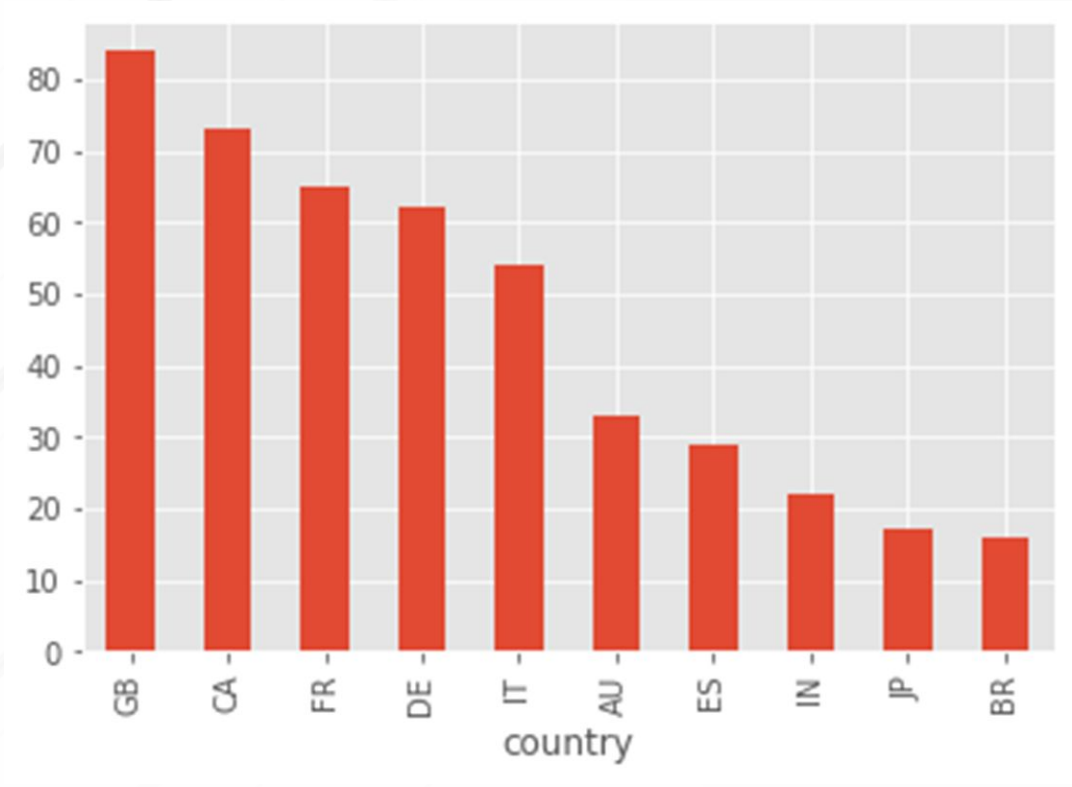
Increase on the number of attacks



Top 10 affected countries in 2021

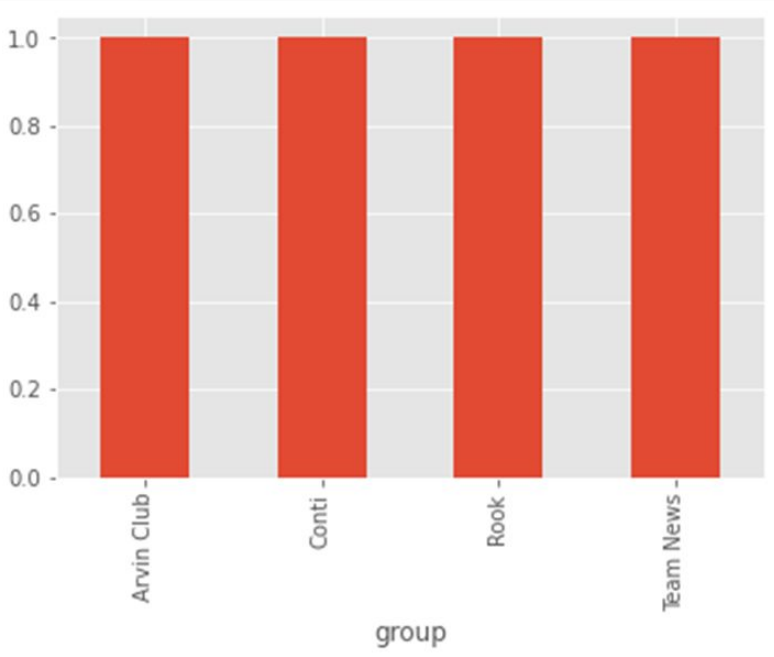


Top 10 affected countries in 2021 – Outside US



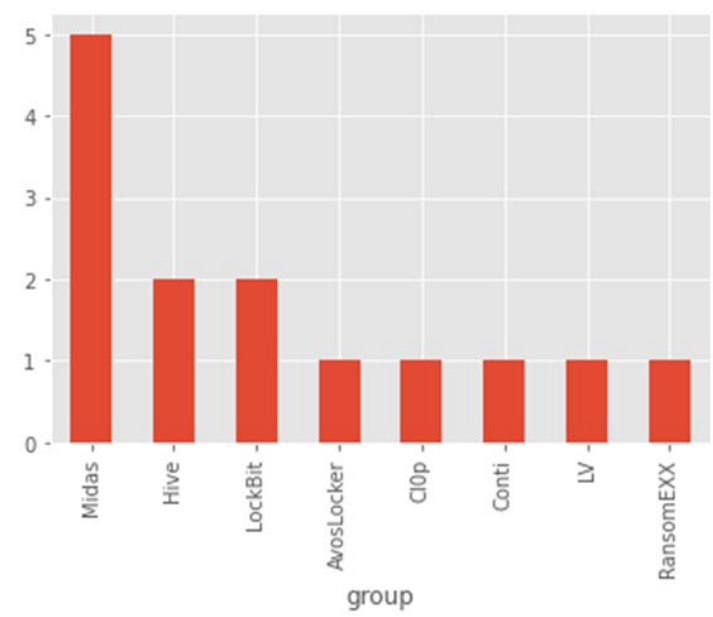
Russian Speaking Countries

company_link	country	sector	group
https://www.kontron.com/en	GE	Information Technology	Conti
http://www.tis-spb.com/	RU	Transportation	Team News
https://www.utair.ru/	RU	Transportation	Arvin Club
https://hcsbk.kz/	KZ	Financial institutions	Rook

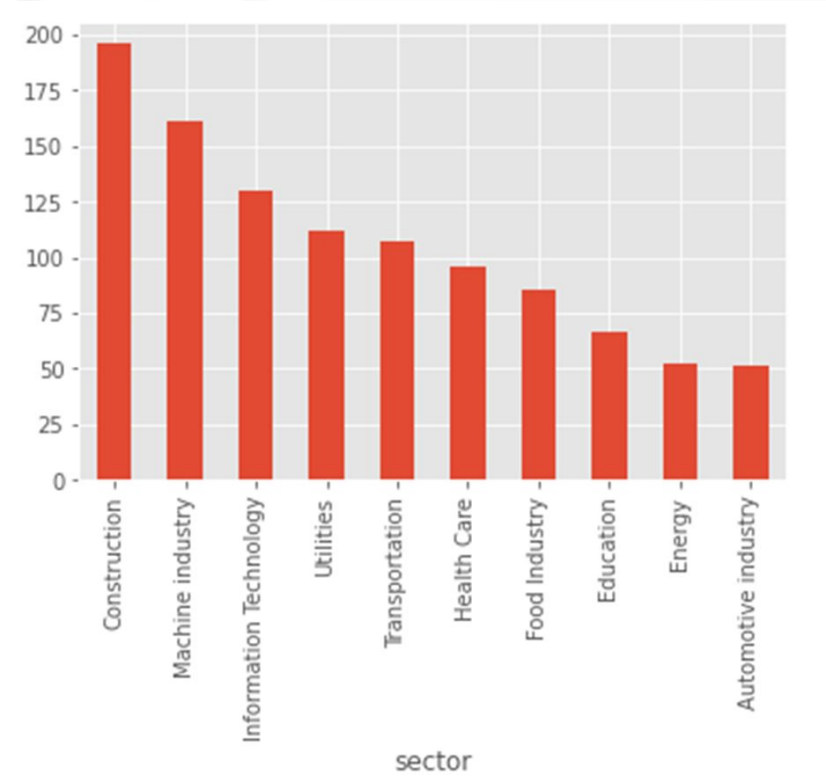


China

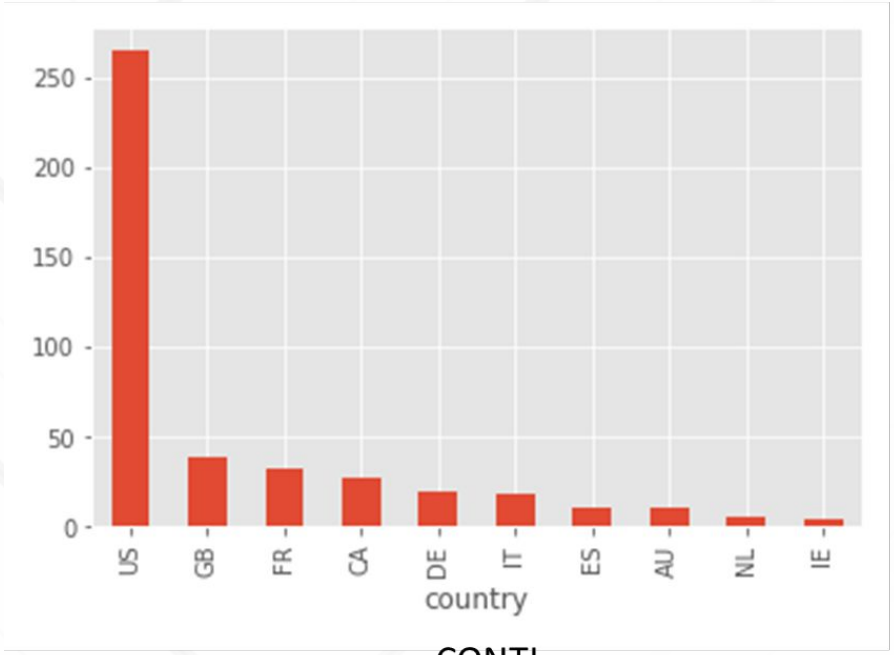
company_link	sector	link	group
http://51talk.com	Education	http://lockbitapt6vx57t3eeqjofv	LockBit
http://isoftstone.com	Information Technology	http://lockbitapt6vx57t3eeqjofv	LockBit
http://www.armchina.com/	Information Technology	http://continewsnv5otx5kaoje7	Conti
http://www.dechang-motor.cor	Machine industry	http://hiveleakdbtnp76ulyhi52e	Hive
http://www.huali-group.com	Utilities	http://avosqxh72b5ia23dl5fgwc	AvosLocker
http://www.shac.com.cn	Automotive industry	http://hiveleakdbtnp76ulyhi52e	Hive
http://www.weichai.com	Machine industry	http://rbvuetuneohce3ouxjlbxt	LV
https://www.walsin.com/	Information Technology	http://rnsm777cdsjrsdlbs4v5qoe	RansomEXX
http://en.epower88.cn/	Energy	http://midasbkic5eyfox4dhnijk	Midas
http://mmoser.com	Construction	http://santat7kpllt6iyvqbr7q4ar	Cl0p
http://www.niell.cn	Energy	http://midasbkic5eyfox4dhnijk	Midas
http://www.shanghai-electric.c	Information Technology	http://midasbkic5eyfox4dhnijk	Midas
http://www1.gewcorp.com/	Energy	http://midasbkic5eyfox4dhnijk	Midas
https://us.imr.cc/companyprofi	Construction	http://midasbkic5eyfox4dhnijk	Midas



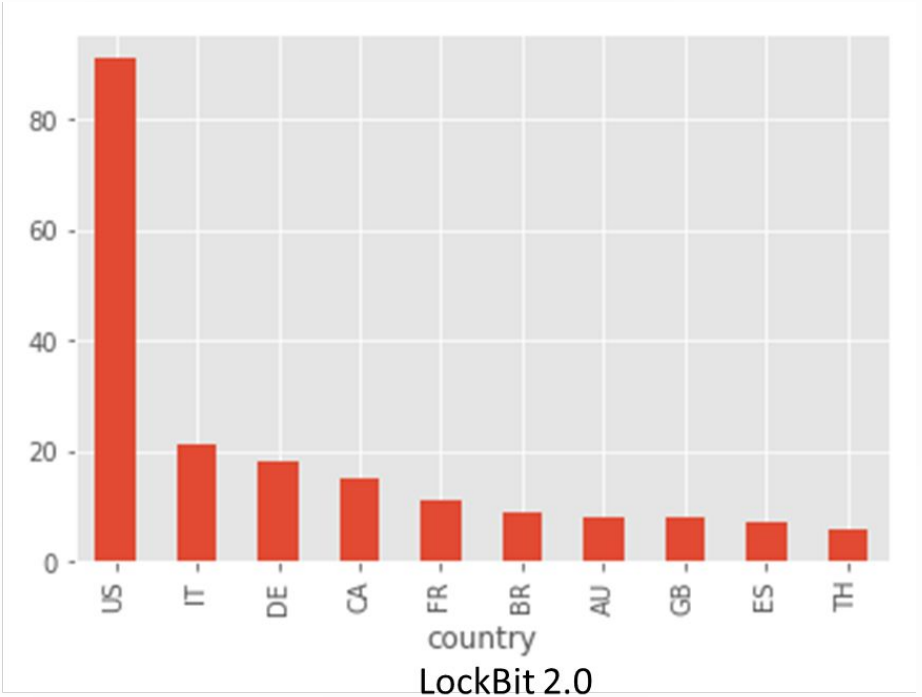
Top 10 affected sectors in 2021



Conti vs LockBit 2.0

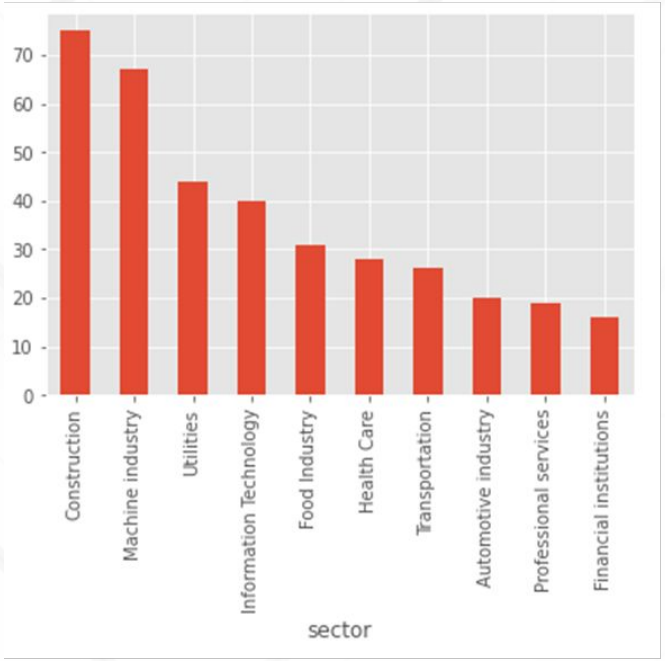


CONTI

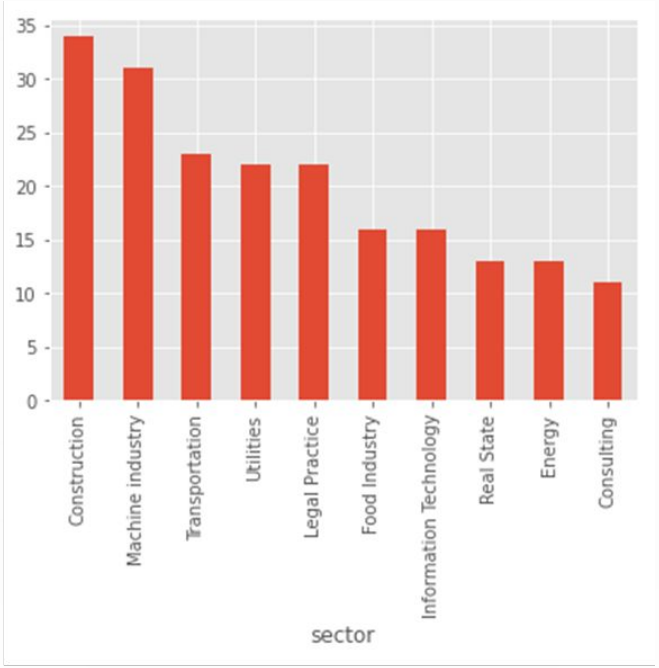


LockBit 2.0

Conti vs LockBit 2.0

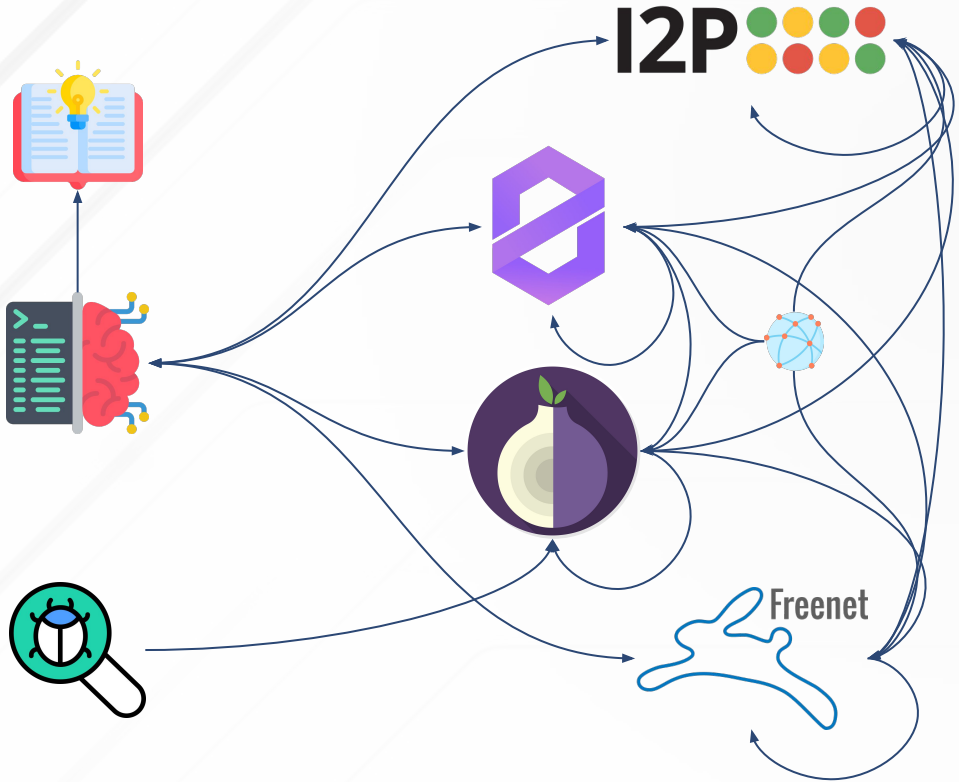


CONTI

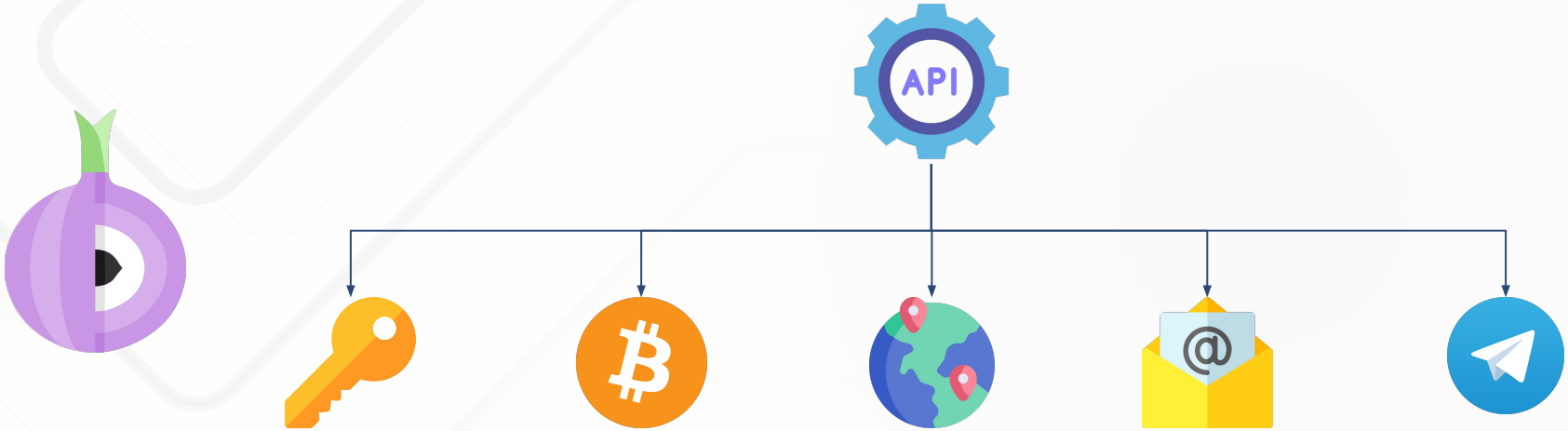


LockBit 2.0

Vysion



Product - Vysion



https://developers.vysion.ai/

Enrichment Results

Below you can see the attributes and objects that are to be created from the results of the enrichment module.

Event ID	1275
Event UUID	540a3112-0115-460a-a73a-26c4542c571c
Event creator org	Testing org
# of resolved Attributes	51 (10 objects)
# of resolved Reports	

Import	Category	Type	Value	Tags	IDS	Disable Correlation	Comment	Distribution
☑	**Name:** vysion-page **References:** 0						banco santander: Enriched via th	Inherit event
☑	Other	**id** text	62a2de29f4b28eceb98eb71f		☐	☐	banco santander: Enriched via th	Inherit event
☑	Network activity	**url** url	http://7tfzrei37r2lkjnycqvra5br4n6dk4a5gfyggfp7ydshugmzkk67apid.onion:80/bank-accounts.html		☑	☐	banco santander: Enriched via th	Inherit event
☑	Other	**network** text	tor		☐	☐	banco santander: Enriched via th	Inherit event
☑	**Name:** vysion-page **References:** 0						banco santander: Enriched via th	Inherit event
☑	Other	**id** text	615483c0b8968e7d85c9b96e		☐	☐	banco santander: Enriched via th	Inherit event
☑	Network activity	**url** url	http://23uudd7qmaq2nu7kvwwwyzqnfyurqicrc26n45afhpwf5qf26drg2vid.onion:80/bank_accounts		☑	☐	banco santander: Enriched via th	Inherit event
☑	Other	**network** text	tor		☐	☐	banco santander: Enriched via th	Inherit event
☑	**Name:** vysion-page **References:** 0						banco santander: Enriched via th	Inherit event
☑	Other	**id** text	616a38e9a72a8244a7a8b3c6		☐	☐	banco santander: Enriched via th	Inherit event
☑	Network activity	**url** url	http://xrlvebokxn22g6x5gmq3cp7rsv3ar5zpirzyqlc4kshwpfnpl2zucdqd.onion:80/node/147712/index.html		☑	☐	banco santander: Enriched via th	Inherit event
☑	Other	**network** text	tor		☐	☐	banco santander: Enriched via th	Inherit event
☑	**Name:** vysion-page **References:** 0						banco santander: Enriched via th	Inherit event
☑	Other	**id** text	619ae8f236275b24ea61fdcf		☐	☐	banco santander: Enriched via th	Inherit event
☑	Network activity	**url** url	http://xrlvebokxn22g6x5gmq3cp7rsv3ar5zpirzyqlc4kshwpfnpl2zucdqd.onion:80/node/147713/index.html		☑	☐	banco santander: Enriched via th	Inherit event
☑	Other	**network** text	tor		☐	☐	banco santander: Enriched via th	Inherit event

Ransomware Feed


```
{
    "data": {
        "total": 5,
        "hits": [
            {
                "id": "690026f1a0b539c23bd51d9e10752fd0fa8ccb399371578b9e73bf068cbc1f7d",
                "company": "PT Astra Honda Motor",
                "company_link": "http://www.astra-honda.com/",
                "link": "http://ecdmr42a34qovoph557zotkfvth4fsz56twvwgiylstjup4r5bpc4oad.onion/JhykowedsgX/UdfGe4kmvb81sp/",
                "group": "Vice Society",
                "date": "2022-06-27T14:17:32",
                "info": " Indonesia  PT Astra Honda Motor is a motorcycle manufacturer based in Jakarta, Indonesia. It is a joint venture between Honda and Astra International. "
            },
            {
                "id": "b2df58acf21cc6abb423857d5c19bc265797be6c4aa1075d079e9dfc9eff8a36",
                "company": "Pilton Community College",
                "company_link": "http://www.piltoncollege.org.uk/",
                "link": "http://ecdmr42a34qovoph557zotkfvth4fsz56twvwgiylstjup4r5bpc4oad.onion/JhykowedsgX/dsW64POGklt8Xx/",
                "group": "Vice Society",
                "date": "2022-06-27T14:17:32",
                "info": " United Kingdom  Pilton Community College is a coeducational secondary school with academy status, located in the Pilton area of Barnstaple in the English county of Devon. "
            },
            {
```

Questions?

carlos.cilleruelo@byronlabs.io | javier.junquera@byronlabs.io

/in/carlos-cilleruelo/ | /in/junquera